Available online at www.sciencedirect.com
ScienceDirect
Journal of Algebra ••• (••••) •••–•••
JOURNAL OF Algebra
www.elsevier.com/locate/jalgebra

Recursively enumerable sets of polynomials over a finite field

Jeroen Demeyer [1]

Universiteit Gent, Vakgroep Zuivere wiskunde en computeralgebra, Galglaan 2, 9000 Gent, Belgium

Received 5 May 2005

Communicated by Laurent Moret-Bailly

Abstract

We prove that a relation over $\mathbb{F}_q[Z]$ is recursively enumerable if and only if it is Diophantine over $\mathbb{F}_q[W, Z]$. We do this by first constructing a model of $\mathbb{N}$ in $\mathbb{F}_q[Z]$, where n is represented by Z^n. In a second step, we show that it suffices to eliminate a bounded universal quantifier. Then finally, the hardest part of the proof is to show that we can eliminate this quantifier.

Keywords: Recursively enumerable sets; Diophantine sets; Hilbert's Tenth Problem; Finite fields

1. Introduction

Hilbert's Tenth Problem (HTP) for a ring $\mathcal{R}$ is the question whether there exists an algorithm to decide whether or not a Diophantine equation has a solution over $\mathcal{R}$. With "Diophantine equation" we mean a polynomial equation with coefficients in $\mathcal{R}$ in any number of variables.

The original question by Hilbert (the 10th from his famous list of 23 problems) was about the integers $\mathbb{Z}$. Hilbert's Tenth Problem for $\mathbb{Z}$ has a negative answer, in the sense that there does not exist an algorithm to decide whether or not a Diophantine equation has a solution over $\mathbb{Z}$. This was proven in 1970 by Yuri Matiyasevič (see [7]), building on earlier work by Martin Davis, Hilary Putnam and Julia Robinson.

E-mail address: jdemeyer@cage.ugent.be.

[1] The author is a Research Assistant of the Fund for Scientific Research—Flanders (Belgium) (F.W.O.-Vlaanderen).

0021-8693/$ – see front matter
doi:10.1016/j.jalgebra.2006.09.030

Please cite this article as: J. Demeyer, Recursively enumerable sets of polynomials over a finite field, J. Algebra (2006), doi:10.1016/j.jalgebra.2006.09.030

Actually, the result was much stronger than just the undecidability of Diophantine equations. They proved that the class of all Diophantine sets is the same as the class of all recursively enumerable sets (see Section 2 for definitions). In what follows, we will refer to this theorem simply as "DPRM." Together with the existence of a set which is recursively enumerable but not recursive, this has as an immediate corollary the negative answer to HTP for $\mathbb{Z}$. In [1], Davis glues together all the older articles, to give a full proof of DPRM from scratch. It was that article which inspired the author to look at $\mathbb{F}_q[Z]$.

While HTP has been settled for a large number of rings (either by proving undecidability, or by giving a decision algorithm), very little is known about the analogue of DPRM: are Diophantine sets over $\mathcal{R}$ the same as recursively enumerable sets over $\mathcal{R}$? Obviously, this question only makes sense if the ring $\mathcal{R}$ is recursive; in particular it has to be countable.

In the cases where $\mathbb{Z}$ is Diophantine in a number ring $\mathcal{O}_K$, one can easily prove the analogue of DPRM for $\mathcal{O}_K$, using the fact that $\mathcal{O}_K$ is a finitely generated $\mathbb{Z}$-module. Denef proved it for $\mathbb{Z}[Z]$ (see [3]) and Zahidi extended this to $\mathcal{O}_K[Z_1, Z_2, \ldots, Z_m]$ with $\mathcal{O}_K$ the ring of integers in a totally real number field (see [12]). To the best of the author's knowledge, this is a complete list of results so far, up to date no results are known in positive characteristic.

In this paper we are looking at the ring $\mathbb{F}_q[Z]$ of polynomials over a finite field. HTP for this ring has a negative answer, as proven by Denef in 1979 (see [4]). He does this by interpreting the integers as Chebyshev polynomials in $\mathbb{F}_q[Z]$. These polynomials are the solutions of a particular Pell equation.

In this paper, we will prove

Main Theorem. *Let p be a prime, and q a power of p. For all $k \geqslant 1$, a subset of $\mathbb{F}_q[Z]^k$ is recursively enumerable if and only if it is Diophantine over $\mathbb{F}_q[W, Z]$ in the language $\mathcal{L} = \{0, 1, +, \cdot, \alpha, W, Z\}$, where $\mathbb{F}_p(\alpha) = \mathbb{F}_q$.*

Note the introduction of a new variable W, which gives us more freedom to make Diophantine definitions. This extra variable is used only in Section 7.3, the rest of the paper just needs the variable Z.

Before the proof of DPRM was completed, Davis and Putnam proved that every recursively enumerable subset of $\mathbb{Z}$ is Diophantine over $\mathbb{Z}[W]$ (see [2]). Our Main Theorem is the analogue of that, but over $\mathbb{F}_q[Z]$ instead of $\mathbb{Z}$.

Eventually, one would like to prove the analogue of DPRM for $\mathbb{F}_q[Z]$, namely that recursively enumerable sets in $\mathbb{F}_q[Z]$ are Diophantine over $\mathbb{F}_q[Z]$. At this point, there is no direct proof of this, but in subsequent work the author will give a Diophantine interpretation of $\mathbb{F}_q[W, Z]$ over $\mathbb{F}_q[Z]$. This uses different techniques than the ones in the present paper. The idea is to encode a polynomial $\sum_i \sum_j \alpha_{ij} W^i Z^j \in \mathbb{F}_q[W, Z]$ as $\sum_i \sum_j \alpha_{ij} Z^{si+j} \in \mathbb{F}_q[Z]$, for a sufficiently large s. Together with the above Main Theorem, this will prove the exact analogue of DPRM.

2. Definitions

We will begin by reviewing the definitions of Diophantine sets and recursively enumerable sets. A very well written introduction to Hilbert's Tenth Problem and the concepts used in this paper can be found in [9]. For a longer survey article and an extensive bibliography, we refer to [8].

Please cite this article as: J. Demeyer, Recursively enumerable sets of polynomials over a finite field, J. Algebra (2006), doi:10.1016/j.jalgebra.2006.09.030

Definition 1. Let $\mathcal{R}$ be a ring (our rings will always be commutative with 1) and k a positive integer. We call a subset $\mathcal{S}$ of $\mathcal{R}^k$ *Diophantine* over $\mathcal{R}$ if and only if there exists a number n and a polynomial $f(a_1, \ldots, a_k, x_1, \ldots, x_n)$ with coefficients in $\mathcal{R}$ such that:

$$\mathcal{S} = \big\{(a_1, \ldots, a_k) \in \mathcal{R}^k \;\big|\; f(a_1, \ldots, a_k, x_1, \ldots, x_n) = 0 \text{ has a solution}\big\}. \tag{1}$$

Usually, we will write this as

$$(a_1, \ldots, a_k) \in \mathcal{S} \quad \Longleftrightarrow \quad (\exists x_1, \ldots, x_n \in \mathcal{R})\ \big(f(a_1, \ldots, a_k, x_1, \ldots, x_n) = 0\big). \tag{2}$$

(1) and (2) are called *Diophantine definitions* of the set $\mathcal{S}$.

In this definition it is important to mention the ring $\mathcal{R}$, since certain sets are Diophantine over one ring, but not over another.

Proposition 1. *Let $\mathcal{R}$ be an integral domain (i.e. there are no zero divisors). Then the union of two Diophantine sets is Diophantine, and if the fraction field of $\mathcal{R}$ is not algebraically closed, then the intersection of two Diophantine sets is also Diophantine.*

Proof. Let $\mathcal{S}_1 \subseteq \mathcal{R}^k$ be defined by the equation $f(a_1, \ldots, a_k, x_1, \ldots, x_m) = 0$, and $\mathcal{S}_2 \subseteq \mathcal{R}^k$ by the equation $g(a_1, \ldots, a_k, y_1, \ldots, y_n) = 0$.

Then it is easy to see that the union $\mathcal{S}_1 \cup \mathcal{S}_2$ is defined by the product

$$f(a_1, \ldots, a_k, x_1, \ldots, x_m) g(a_1, \ldots, a_k, y_1, \ldots, y_n) = 0. \tag{3}$$

For the intersection, we need a polynomial $h(x) = \sum_{i=0}^{d} a_i x^i \in \mathcal{R}[x]$ with $d > 0$ and $a_d \neq 0$, which has no roots in the fraction field of $\mathcal{R}$. Such a polynomial exists, because we assumed that this field is not algebraically closed. We claim that $\mathcal{S}_1 \cap \mathcal{S}_2$ is defined by

$$\sum_{i=0}^{d} a_i f(a_1, \ldots, a_k, x_1, \ldots, x_m)^{d-i} g(a_1, \ldots, a_k, y_1, \ldots, y_n)^i = 0. \tag{4}$$

It is clear that a solution to $f = 0$ and $g = 0$ gives a solution to (4).

Conversely, suppose (4) has a solution $x_1, \ldots, x_m, y_1, \ldots, y_n$. Then

$$0 = f(\bar{a}, \bar{x})^d \sum_{i=0}^{d} a_i \frac{g(\bar{a}, \bar{y})^i}{f(\bar{a}, \bar{x})^i} = f(\bar{a}, \bar{x})^d h\left(\frac{g(\bar{a}, \bar{y})}{f(\bar{a}, \bar{x})}\right).$$

Since h has no zeros, $f(\bar{a}, \bar{x})$ must be zero, and the only term remaining in (4) is $a_d g(\bar{a}, \bar{y})^d = 0$, which implies $g(\bar{a}, \bar{y}) = 0$. So we see that $f(\bar{a}, \bar{x}) = g(\bar{a}, \bar{y}) = 0$, which means that we just defined the intersection of $\mathcal{S}_1$ and $\mathcal{S}_2$. □

In what follows, we will write down Diophantine definitions with existential quantifiers ("there exists," $\exists$), as in formula (2). In this notation, intersections correspond with logical conjunctions ("and," $\wedge$), and unions with logical disjunctions ("or," $\vee$). All the rings we encounter

Please cite this article as: J. Demeyer, Recursively enumerable sets of polynomials over a finite field, J. Algebra (2006), doi:10.1016/j.jalgebra.2006.09.030

will satisfy the conditions of the preceding proposition, so we can write $\wedge$ and $\vee$ as many times as we like in our Diophantine definitions.

Throughout this paper, we will write $\mathbb{N}$ for the set of non-negative integers $\{0, 1, 2, \ldots\}$.

Definition 2. Let $\mathcal{S}$ be a subset of $\mathbb{N}^k$.

- $\mathcal{S}$ is called *recursively enumerable* (r.e.) if there exists an algorithm which lists exactly the set $\mathcal{S}$. This algorithm can run forever, but every element of $\mathcal{S}$ has to be printed at least once.
- $\mathcal{S} \subseteq \mathbb{N}^k$ is *recursive* if there exists an algorithm, which on input $x \in \mathbb{N}^k$, decides whether or not $x \in \mathcal{S}$. It is easy to see that a set $\mathcal{S}$ is recursive if and only if both $\mathcal{S}$ and its complement are recursively enumerable.

If we want to extend the above notions of recursively enumerable and recursive sets to other rings, we require the ring to be recursive.

Definition 3. A *recursive ring* (also called *computable ring* or *explicit ring*) $\mathcal{R}$ is a countable ring admitting an injection $\theta : \mathcal{R} \hookrightarrow \mathbb{N}$ such that $\operatorname{Im}\theta$ is recursive (as a subset of $\mathbb{N}$) and both

$$\big\{\big(\theta(X), \theta(Y), \theta(X+Y)\big) \bigm| X, Y \in \mathcal{R}\big\} \quad \text{and} \quad \big\{\big(\theta(X), \theta(Y), \theta(XY)\big) \bigm| X, Y \in \mathcal{R}\big\}$$

are recursive subsets of $\mathbb{N}^3$. We call θ a *recursive presentation* of $\mathcal{R}$. More background on this can be found in [5] or [10].

Definition 4. Let $\mathcal{R}$ be a recursive ring with recursive presentation $\theta : \mathcal{R} \hookrightarrow \mathbb{N}$. A subset $\mathcal{S}$ of $\mathcal{R}^k$ is said to be r.e. (respectively recursive) if the component-wise image of $\mathcal{S}$ under θ is an r.e. (respectively recursive) subset of $\mathbb{N}^k$.

A problem with these definitions is that the recursive presentation θ is far from unique, so a certain set $\mathcal{S} \subseteq \mathcal{R}^k$ could be r.e. for one presentation θ_1, but not for another θ_2. However, for the rings we work with, namely $\mathbb{F}_q[Z]$, $\mathbb{F}_q[W, Z]$ and $\mathbb{Z}$, all possible recursive presentations are equivalent, in the sense that they give the same r.e. and recursive sets (see [5], in particular Theorem 3.1).

3. Strategy

As mentioned in the introduction, there is the well-known Davis–Putnam–Robinson–Matiyasevič Theorem:

Theorem 1 *(DPRM). For all $k \geqslant 1$, a subset of $\mathbb{Z}^k$ is recursively enumerable if and only if it is Diophantine over $\mathbb{Z}$.*

We need to remark that this proof actually worked in $\mathbb{Z}_{\geqslant 1}$ instead of $\mathbb{Z}$, but this does not matter since $\mathbb{Z}_{\geqslant 1}$ is Diophantine over $\mathbb{Z}$ (something is positive if and only if it is a sum of 4 squares plus 1) and there is a model of $\mathbb{Z}$ in $\mathbb{Z}_{\geqslant 1}^2$ (represent an integer as a difference of positive numbers). In this paper, we work over $\mathbb{N} = \mathbb{Z}_{\geqslant 0}$, which is essentially the same (elements of $\mathbb{Z}_{\geqslant 0}$ are a sum of 4 squares).

As said in the introduction, our Main Theorem will be the following.

Please cite this article as: J. Demeyer, Recursively enumerable sets of polynomials over a finite field, J. Algebra (2006), doi:10.1016/j.jalgebra.2006.09.030

Main Theorem. *Let p be a prime, and q a power of p. For all $k \geqslant 1$, a subset of $\mathbb{F}_q[Z]^k$ is recursively enumerable if and only if it is Diophantine over $\mathbb{F}_q[W, Z]$ in the language $\mathcal{L} = \{0, 1, +, \cdot, \alpha, W, Z\}$, where $\mathbb{F}_p(\alpha) = \mathbb{F}_q$.*

Both for the original DPRM Theorem, as well as for this theorem, the "if" direction is immediate: Let $\mathcal{R}$ be any recursive ring. It is easy to see that every Diophantine subset of $\mathcal{R}^k$ is r.e.: take a Diophantine set

$$\mathcal{S} = \big\{(a_1, \ldots, a_k) \in \mathcal{R}^k \;\big|\; f(a_1, \ldots, a_k, x_1, \ldots, x_n) = 0 \text{ has a solution}\big\}.$$

Construct an algorithm which simply tries all possible values for $(a_1, \ldots, a_k, x_1, \ldots, x_n) \in \mathcal{R}^{k+n}$, and prints $(a_1, \ldots, a_k)$ whenever a zero of f is found. This algorithm will list exactly the set $\mathcal{S}$.

The hard part is the "only if" direction of the Main Theorem. The first thing we need to do is to construct a Diophantine model of $\mathbb{N}$ in $\mathbb{F}_q[Z]$ (see Section 4), by mapping a natural number $n \geqslant 0$ to the polynomial Z^n. This model is strongly based on Denef's model for $\mathbb{Z}$ in $\mathbb{F}_q[Z]$ (see [4]). The construction of the model is the only place where we must distinguish between odd and even characteristic.

Given this model of $\mathbb{N}$ in $\mathbb{F}_q[Z]$, the most difficult part of this paper is the elimination of bounded universal quantifiers (see Section 7). Such a quantifier, written $(\forall k)_{\leqslant y}$, means "for $k = 0, 1, \ldots, y$." Here, k and y are natural numbers, represented by Z^k and Z^y in the model. Given a formula with a bounded universal quantifier (and any number of existential quantifiers), we have to show that it is equivalent to a formula with only existential quantifiers. This is the part where the variable W is needed, to make certain Diophantine definitions.

The elimination of bounded universal quantifiers was also one of the key components needed in the proof of DPRM (see [1, pp. 252–256]). There, each of the y formulas arising from the bounded universal quantifier $(\forall k)_{\leqslant y}$ is considered modulo a different large number in an arithmetic progression, and then these y formulas are encoded into just one formula using the Chinese Remainder Theorem. Our method also uses the Chinese Remainder Theorem, but modulo a product of certain cyclotomic polynomials, instead of numbers in an arithmetic progression. Apart from this idea of using the Chinese Remainder Theorem, there is very little in the DPRM proof which works for $\mathbb{F}_q[Z]$.

Once we know how to eliminate bounded universal quantifiers, the rest of the proof is easy to fill in. A classical method to prove analogues of DPRM is to reduce to $\mathbb{N}$, where it is known that r.e. sets are Diophantine. To do this, we have to enumerate $\mathbb{F}_q[Z]$ as $\{P^{(0)}, P^{(1)}, P^{(2)}, \ldots\}$, where $P^{(n)}$ is seen as the nth polynomial in $\mathbb{F}_q[Z]$. By a standard argument (see Section 6.1), it suffices to prove that the relation "X is the nth polynomial," with X in $\mathbb{F}_q[Z]$, is Diophantine over $\mathbb{F}_q[W, Z]$.

Defining this relation can be done using a bounded universal quantifier, where the bound is the degree of the polynomial $P^{(n)}$ to be defined (see Section 6.2). A quantifier $(\forall k)_{\leqslant d}$ gives $d + 1$ values for k. And a polynomial of degree d has $d + 1$ coefficients, so we just need to express that the degree of X is (at most) d, and that the kth coefficient of X equals the kth coefficient of $P^{(n)}$ for all $k \leqslant d$.

4. A model of $\mathbb{N}$ in $\mathbb{F}_q[W, Z]$

In this section, we will construct models of $\mathbb{N} = \{0, 1, 2, \ldots\}$ where $n \in \mathbb{N}$ corresponds with T^n in $\mathbb{F}_q[W, Z]$. We can make such a model for every non-constant polynomial T (this means

Please cite this article as: J. Demeyer, Recursively enumerable sets of polynomials over a finite field, J. Algebra (2006), doi:10.1016/j.jalgebra.2006.09.030

$T \in \mathbb{F}_q[W, Z] \setminus \mathbb{F}_q$). In [4], Denef constructs a model of $\mathbb{Z}$ in $\mathbb{F}_q[Z]$, using the Chebyshev polynomials. Ours differs from his, but we do need many of his ideas to construct our model. Just like in Denef's paper, we have to make the distinction between odd and even characteristic.

4.1. Odd characteristic

In the case p is odd, we will use the Chebyshev polynomials $X_n, Y_n \in \mathbb{Z}[Z]$. These are defined by

$$\left(Z + \sqrt{Z^2 - 1}\right)^n = X_n(Z) + \sqrt{Z^2 - 1}\, Y_n(Z) \quad (n \in \mathbb{Z}).$$

Note that $(Z+\sqrt{Z^2-1})^{-1} = (Z-\sqrt{Z^2-1})$, so this definition also makes sense for negative n.

The couples (X_n, Y_n) are solutions of the Pell equation

$$X^2 - \left(Z^2 - 1\right)Y^2 = 1. \tag{5}$$

We can see them as elements of $\mathbb{F}_q[Z]$ by reducing the coefficients modulo p.

Facts 1. *These are some easy facts about the Chebyshev polynomials* (*see for instance* [4]). *They are true in all polynomial rings of characteristic not* 2.

$$\begin{aligned}
&X_0 = 1, && Y_0 = 0,\\
&X_1 = Z, && Y_1 = 1,\\
&X_{n+k} = X_n X_k + \left(Z^2 - 1\right) Y_n Y_k, && Y_{n+k} = X_n Y_k + Y_n X_k,\\
&X_{-n} = X_n, && Y_{-n} = -Y_n,\\
&\deg X_n = n \quad (n \geqslant 0), && \deg Y_n = n - 1 \quad (n \geqslant 1).
\end{aligned}$$

Proposition 2 *(Pell equation). Let T, X and Y be elements of $\mathbb{F}_q[W, Z]$, with T non-constant. Then*

$$(\exists n \in \mathbb{Z})\ \left(X = X_n(T) \wedge Y = Y_n(T)\right) \quad \Longleftrightarrow \quad \left(X^2 - \left(T^2 - 1\right)Y^2 = 1 \wedge T - 1 | X - 1\right).$$

Proof. This follows from [4, p. 137, (4)–(5)], applied to either the ring $\mathbb{F}_q[W]$ or $\mathbb{F}_q[Z]$. □

Proposition 3. *Let A and B be elements of $\mathbb{F}_q[W, Z]$ with B non-constant. Then*

$$\begin{aligned}
&(\exists k \in \mathbb{N})\ \left(A = B^{p^k}\right)\\
&\quad \Longleftrightarrow \quad (\exists m \in \mathbb{Z})\ \left(A = X_m(B)\right) \wedge (\exists n \in \mathbb{Z})\ \left(A + 1 = X_n(B + 1)\right).
\end{aligned}$$

Proof. The direction "⇒" follows from the fact that $X_{p^k} = Z^{p^k}$, hence $X_{p^k}(T) = T^{p^k}$.

Conversely, from the right-hand side of the equivalence follows that

$$X_m(B) + 1 = X_n(B + 1).$$

Please cite this article as: J. Demeyer, Recursively enumerable sets of polynomials over a finite field, J. Algebra (2006), doi:10.1016/j.jalgebra.2006.09.030

Considering degrees, we see that m and n have to be equal. Now the statement follows from Lemma 2.1 point 6 in [4]. □

Proposition 4. *Let $T \in \mathbb{F}_q(W, Z)^*$ and $n \in \mathbb{Z}$. Then the following equality holds*:

$$T^n = X_n\left(\frac{T+T^{-1}}{2}\right) + \frac{T-T^{-1}}{2} Y_n\left(\frac{T+T^{-1}}{2}\right). \tag{6}$$

Proof. We prove this by induction on n, using Facts 1. The statement clearly holds for $n = 0$, because $X_0 = 1$ and $Y_0 = 0$. For n positive, we will expand the right-hand side of (6). For ease of notation, we omit the arguments of the Chebyshev polynomials, they are always $\frac{T+T^{-1}}{2}$.

$$\begin{aligned}
&X_n + \frac{T-T^{-1}}{2} Y_n \\
&\quad = X_1 X_{n-1} + \left(\left(\frac{T+T^{-1}}{2}\right)^2 - 1\right) Y_1 Y_{n-1} + \frac{T-T^{-1}}{2} X_1 Y_{n-1} + \frac{T-T^{-1}}{2} Y_1 X_{n-1} \\
&\quad = \frac{T+T^{-1}}{2} X_{n-1} + \frac{T^2-2+T^{-2}}{4} Y_{n-1} + \frac{T^2-T^{-2}}{4} Y_{n-1} + \frac{T-T^{-1}}{2} X_{n-1} \\
&\quad = T X_{n-1} + \frac{T^2-1}{2} Y_{n-1} = T\left(X_{n-1} + \frac{T-T^{-1}}{2} Y_{n-1}\right).
\end{aligned}$$

The proposition for negative n follows by exchanging the roles of T and T^{-1}, and by the fact that $X_{-n} = X_n$ and $Y_{-n} = -Y_n$. □

Using Proposition 4, we will define a model of $\mathbb{N}$ in $\mathbb{F}_q[W, Z]$. We cannot apply (6) directly to define T^n, because we need T^{-1}, which is not a polynomial. Instead, we will define powers modulo a particular polynomial.

Proposition 5. *Let T be a non-constant polynomial in $\mathbb{F}_q[W, Z]$. Then we can give a Diophantine definition of the powers of T as follows*:

$$(\exists n \in \mathbb{N})\ \left(A = T^n\right) \tag{7}$$

$$\Updownarrow$$

$$\left(\exists S, X, Y \in \mathbb{F}_q[W, Z]\right)$$

$$(\exists k \in \mathbb{N})\ \left(S = T^{p^k}\right) \tag{8}$$

$$\wedge\ (\exists n \in \mathbb{Z})\ \left(X = X_n\left(\frac{T+S}{2}\right) \wedge Y = Y_n\left(\frac{T+S}{2}\right)\right) \tag{9}$$

$$\wedge\ A \equiv X + \frac{T-S}{2} Y \mod TS - 1 \tag{10}$$

$$\wedge\ A | S. \tag{11}$$

Please cite this article as: J. Demeyer, Recursively enumerable sets of polynomials over a finite field, J. Algebra (2006), doi:10.1016/j.jalgebra.2006.09.030

Proof. Suppose that $A = T^n$. Take a k such that $n \leqslant p^k$, and let S be T^{p^k}. Set $X = X_n(\frac{T+S}{2})$ and $Y = Y_n(\frac{T+S}{2})$. This already gives (8), (9) and (11). Now S is the inverse of T modulo $TS - 1$, so Proposition 4 implies (10).

Conversely, assume (8) to (11) hold. From (9) and (10) it follows that $A \equiv T^m \mod TS - 1$ for a certain $m \in \mathbb{Z}$. Since $S = T^{p^k}$, we have $T^{p^k+1} \equiv 1 \mod TS - 1$. Let n be the unique integer such that $0 \leqslant n \leqslant p^k$ and $n \equiv m \mod p^k + 1$. This implies that

$$A \equiv T^n \mod TS - 1. \tag{12}$$

If we can prove that $\deg A < \deg(TS - 1)$ and $\deg T^n < \deg(TS - 1)$, it will follow that A is equal to T^n. We know that $\deg A \leqslant \deg S = p^k \deg T$ because A divides S. But also $\deg T^n = n \deg T$. Both these degrees are less than $\deg(TS - 1) = (p^k + 1)\deg T$. □

4.2. Even characteristic

This will be very analogous to the case p odd, we just need to change the equations somewhat. In characteristic 2, the usual Pell equation $X^2 - (T^2 - 1)Y^2 = 1$ is equivalent to $X - (T - 1)Y = 1$, so we must use a different equation.

Let α be a root of

$$\alpha^2 + Z\alpha + 1 = 0.$$

Then we define the polynomials $X_n, Y_n \in \mathbb{F}_2[Z]$ as

$$\alpha^n = X_n(Z) + \alpha Y_n(Z).$$

These are solutions of

$$X^2 + ZXY + Y^2 = 1.$$

These X_n and Y_n have properties very analogous to the Chebyshev polynomials. We will not give any proofs since they are practically the same as in the case p odd. Again, we refer to [4].

Facts 2.

$$\begin{aligned}
&X_0 = 1, && Y_0 = 0,\\
&X_1 = 0, && Y_1 = 1,\\
&X_{n+k} = X_nX_k + Y_nY_k, && Y_{n+k} = X_nY_k + Y_nX_k + ZY_nY_k,\\
&X_{-n} = X_n + ZY_n, && Y_{-n} = Y_n,\\
&\deg X_n = n - 2 \quad (n \geqslant 2), && \deg Y_n = n - 1 \quad (n \geqslant 1).
\end{aligned}$$

Proposition 6. *Let T, X and Y be elements of $\mathbb{F}_q[W, Z]$, with T non-constant. Then*

$$(\exists n \in \mathbb{Z})\ \big(X = X_n(T) \wedge Y = Y_n(T)\big) \quad \Longleftrightarrow \quad \big(X^2 + ZXY + Y^2 = 1\big).$$

Please cite this article as: J. Demeyer, Recursively enumerable sets of polynomials over a finite field, J. Algebra (2006), doi:10.1016/j.jalgebra.2006.09.030

Proposition 7. *Let A and B be elements of $\mathbb{F}_q[W, Z]$ with B non-constant. Then*

$$(\exists k \in \mathbb{N})\ \left(A = B^{2^k}\right)$$
$$\iff \quad (\exists m \in \mathbb{Z})\ \left(A = B \cdot Y_m(B)\right) \wedge (\exists n \in \mathbb{Z})\ \left(A + 1 = (B+1) \cdot Y_n(B+1)\right).$$

Proposition 8. *Let $T \in \mathbb{F}_q(W, Z)^*$ and $n \in \mathbb{Z}$. Then the following equality holds*:

$$T^n = X_n\left(T + T^{-1}\right) + T Y_n\left(T + T^{-1}\right). \tag{13}$$

Proposition 9. *Let T be a non-constant polynomial in $\mathbb{F}_q[W, Z]$. Then we can give a Diophantine definition of the powers of T as follows*:

$$(\exists n \in \mathbb{N})\ \left(A = T^n\right) \tag{14}$$
$$\Updownarrow$$
$$\left(\exists S, X, Y \in \mathbb{F}_q[W, Z]\right)$$
$$(\exists k \in \mathbb{N})\ \left(S = T^{2^k}\right) \tag{15}$$
$$\wedge\ (\exists n \in \mathbb{Z})\ \left(X = X_n(T + S) \wedge Y = Y_n(T + S)\right) \tag{16}$$
$$\wedge\ A \equiv X + TY \mod TS - 1 \tag{17}$$
$$\wedge\ A | S. \tag{18}$$

4.3. Operators

So far, we defined the set of powers of T, where T was any non-constant polynomial. It is convenient that we got the same result for odd and even characteristic. This will allow us to forget about characteristic in the remainder of this paper.

In order to have a Diophantine model, we must also give Diophantine definitions of addition and multiplication. Addition is trivial, because $T^{a+b} = T^a T^b$.

Instead of defining multiplication directly, we use a trick by Denef. Let $|$ denote the usual divisibility in $\mathbb{N}$ and define the relation $|^p$ as

$$a|^p b \quad \iff \quad (\exists k \in \mathbb{N})\ \left(b = p^k a\right).$$

Then multiplication can be defined in $\langle \mathbb{N}, +, |, |^p \rangle$ (see [4]). So, in order to have a model of $\langle \mathbb{N}, +, \cdot \rangle$ in $\langle \mathbb{F}_q[W, Z], +, \cdot \rangle$, we just need to define the relations $|$ and $|^p$ in this model. This can be done in a Diophantine way as follows:

$$a|b \quad \iff \quad T^a - 1 | T^b - 1,$$
$$a|^p b \quad \iff \quad (\exists k)\ \left(\left(T^a\right)^{p^k} = T^b\right).$$

Please cite this article as: J. Demeyer, Recursively enumerable sets of polynomials over a finite field, J. Algebra (2006), doi:10.1016/j.jalgebra.2006.09.030

4.4. The model

We have defined infinitely many models of $\mathbb{N}$ in $\mathbb{F}_q[W, Z]$. Indeed, we have a model for every T in $\mathbb{F}_q[W, Z] \setminus \mathbb{F}_q$. But we will almost exclusively work with one particular model, namely the one with $T = Z$. So, a natural number $n \in \mathbb{N}$ corresponds to $Z^n \in \mathbb{F}_q[W, Z]$.

This leads to two types of variables: The first type will be written with Latin uppercase letters ($A, B, \ldots$), and run in $\mathbb{F}_q[W, Z]$. The second type, denoted with Latin lowercase letters ($a, b, \ldots$), run in $\mathbb{N}$, but are represented by powers of Z.

If we write down a formula mixing these two types, the variables of the second type can only occur as powers of Z. Consider, as an example, the formula

$$(\exists n \in \mathbb{N})\ \big((Z-1)A = Z^n - 1\big).$$

This really means

$$\big(\exists X \in \mathbb{F}_q[W, Z]\big)\ \big((\exists n \in \mathbb{N})\ \big(X = Z^n\big) \wedge \big((Z-1)A = X - 1\big)\big).$$

The part $(\exists n \in \mathbb{N})\ (X = Z^n)$ is Diophantine as shown above, so the whole formula is Diophantine.

Sometimes we will write down formulas containing only variables of the second type (natural numbers). An example of this could be

$$(\exists a \in \mathbb{N})\ \big(a \text{ is prime} \wedge n = m^a - 1\big).$$

When we see all variables in this formula as natural numbers, it is Diophantine over $\mathbb{N}$, by DPRM. As we encode these variables as powers of Z, the resulting relation between Z^n and Z^m is Diophantine over $\mathbb{F}_q[W, Z]$ because our model of $\mathbb{N}$ is Diophantine.

4.5. Defining arbitrary powers

The purpose of this section is to prove that B^n is a Diophantine function of B and n. Remember that n is being represented by Z^n, so we should say a function of B and Z^n.

We will do this in two steps: first we do the case where n is a power of the characteristic p. Then we will do arbitrary n, but only in the case that $B \neq 0$, which is sufficient for our purposes.

Proposition 10. *Let $A, B \in \mathbb{F}_q[W, Z]$ and $h \in \mathbb{N}$. Then the relation "$A = B^{p^h}$" between A, B and Z^{p^h} is Diophantine*:

$$A = B^{p^h} \tag{19}$$

$$\Updownarrow$$

$$(\exists k \in \mathbb{N})\ \big(A \cdot \big(Z^{p^h}\big)^2 + Z^{p^h} = \big(BZ^2 + Z\big)^{p^k}\big). \tag{20}$$

Remark. Formula (20) is Diophantine by either Proposition 3 (for $p > 2$) or 7 (for $p = 2$). The condition that $BZ^2 + Z$ is non-constant is indeed satisfied.

Please cite this article as: J. Demeyer, Recursively enumerable sets of polynomials over a finite field, J. Algebra (2006), doi:10.1016/j.jalgebra.2006.09.030

Proof. If $A = B^{p^h}$, then clearly (20) holds with $k = h$.

Conversely, assume (20). Then we have for a certain k that

$$AZ^{2p^h} + Z^{p^h} = B^{p^k} Z^{2p^k} + Z^{p^k}. \tag{21}$$

The order at $Z = 0$ of the left-hand side is p^h, the right-hand side has order p^k. These have to be equal, so $k = h$ and it follows immediately from (21) that $A = B^{p^k} = B^{p^h}$. □

Now we can also define general powers (for technical reasons, we add the condition $B \neq 0$):

Proposition 11. *Let $A, B \in \mathbb{F}_q[W, Z]$ and $n \in \mathbb{N}$ with $B \neq 0$. Then*

$$A = B^n \tag{22}$$

$$\Updownarrow$$

$$\big(\exists C \in \mathbb{F}_q[W, Z]\big)\ (\exists m \in \mathbb{N})$$

$$m = p^n \tag{23}$$

$$\wedge\ C = B^m \tag{24}$$

$$\wedge\ (\exists k \in \mathbb{N})\ \big(AZ^n = (BZ)^k \wedge CZ^m = (BZ)^{p^k}\big). \tag{25}$$

Remark. In the preceding proposition, we proved that (24) is Diophantine. (23) is Diophantine by DPRM. As for formula (25), saying that AZ^n and CZ^m are both powers of BZ is Diophantine. But (25) also gives a relation between these powers. Using the Diophantine model of $\mathbb{N}$ in $\mathbb{F}_q[W, Z]$ where n corresponds to $(BZ)^n$, we see that this relation between AZ^n and CZ^m is Diophantine, since it is recursive.

Proof. Immediate. □

4.6. Bounding degree

A frequently used technique in our Diophantine definitions is to combine a congruence with a bound. The idea is the following: suppose we know that $A \equiv B \bmod C$ for certain polynomials A, B and C. If we can prove that $\deg A < \deg C$ and $\deg B < \deg C$, then we may conclude that $A = B$. We already used this technique on (12) in Proposition 5.

Congruences are Diophantine, but we still need a Diophantine way to bound degrees. Unfortunately, we can do this only for polynomials in one variable Z. If a similar bound could be made for polynomials in the two variables, then it would follow that r.e. sets in $\mathbb{F}_q[W, Z]$ (as opposed to $\mathbb{F}_q[Z]$) are Diophantine over $\mathbb{F}_q[W, Z]$.

Definition 5. Define the following Diophantine predicate:

$$\beta(X, e) \quad \Longleftrightarrow \quad X = 0 \vee \big(X | Z^{q^{2e}} - Z^{q^e}\big).$$

Equivalently,

$$\beta(X, e) \quad \Longleftrightarrow \quad X^2 \big| \big(Z^{q^{2e}} - Z^{q^e}\big) X.$$

Please cite this article as: J. Demeyer, Recursively enumerable sets of polynomials over a finite field, J. Algebra (2006), doi:10.1016/j.jalgebra.2006.09.030

Given an $X \in \mathbb{F}_q[Z]$ for which $\beta(X, e)$ holds, necessarily $\deg X \leqslant q^{2e}$ (adopting the convention that $\deg 0 = -\infty$).

Lemma 3. *For every polynomial $X \in \mathbb{F}_q[Z]$ there exists an e such that $\beta(X, e)$.*

Proof. For $X = 0$, the statement is clear, so assume $X \neq 0$. Let Y be the biggest squarefree divisor (the radical) of X, then there exists a c for which $X | Y^c$. Because Y is non-zero and squarefree, it will have a finite number of roots, all distinct. Let $\mathbb{F}_{q^d}$ be a field containing all these roots, then

$$Y \Big| \prod_{\xi \in \mathbb{F}_{q^d}} (Z - \xi) = Z^{q^d} - Z.$$

If we take $e \in \mathbb{N}$ such that $d | e$ and $c \leqslant q^e$, we get

$$X \big| Y^c \big| Y^{q^e} \big| \big(Z^{q^d} - Z\big)^{q^e} \big| \big(Z^{q^e} - Z\big)^{q^e} = Z^{q^{2e}} - Z^{q^e}.$$

This means that $\beta(X, e)$ will be true. □

Corollary 12. *For every finite set of polynomials $X_1, \ldots, X_n \in \mathbb{F}_q[Z]$, there exists an e such that $\beta(X_i, e)$ holds for all $1 \leqslant i \leqslant n$.*

Proof. Since $\beta(0, e)$ is always true, we may assume without loss of generality that none of the given polynomials equals zero. Now apply the preceding lemma on $X = X_1 X_2 \ldots X_n$. Since $X \neq 0$, this will give us an e such that $X_i | X | Z^{q^{2e}} - Z^{q^e}$ for all $1 \leqslant i \leqslant n$. □

Definition 6. Define the following sequence of finite subsets of $\mathbb{F}_q[Z]$:

$$\begin{aligned} \mathcal{B}_u &= \big\{ X \in \mathbb{F}_q[Z] \;\big|\; \beta(X, u) \big\} \\ &= \big\{ X \in \mathbb{F}_q[Z] \;\big|\; X = 0 \;\vee\; X | Z^{q^{2u}} - Z^{q^u} \big\}. \end{aligned}$$

From the corollary it follows that every finite subset of $\mathbb{F}_q[Z]$ is contained in at least one $\mathcal{B}_u$. Every finite subset will even be contained in infinitely many different $\mathcal{B}_u$, since $\mathcal{B}_u \subset \mathcal{B}_v$ whenever $u | v$.

So we see that we can use the predicate $\beta(\cdot, e)$ to 'bound' the degree of a polynomial. But β also serves another purpose, namely to Diophantinely define the set $\mathbb{F}_q[Z]$ in $\mathbb{F}_q[W, Z]$:

Lemma 4. *For $X \in \mathbb{F}_q[W, Z]$ we have*

$$X \in \mathbb{F}_q[Z] \quad \Longleftrightarrow \quad X = 0 \vee (\exists e) \left(X | Z^{q^{2e}} - Z^{q^e} \right).$$

Proof. The "⇒" direction is essentially what we proved in Lemma 3. "⇐" is immediately clear: a polynomial involving W can never be a divisor of a polynomial in the variable Z. □

Please cite this article as: J. Demeyer, Recursively enumerable sets of polynomials over a finite field, J. Algebra (2006), doi:10.1016/j.jalgebra.2006.09.030

5. Cyclotomic polynomials

In the rest of this paper, we will often work with cyclotomic polynomials. To define the nth cyclotomic polynomial $\Phi_n \in \mathbb{Q}[Z]$, consider ζ_n, a primitive nth root of unity in some number field. Then Φ_n is defined as the minimal polynomial of ζ_n, or

$$\Phi_n(Z) = \prod_{k \in (\mathbb{Z}/n\mathbb{Z})^*} \left(Z - \zeta_n^k\right).$$

We see that Φ_n is monic of degree $\varphi(n)$, where φ denotes the Euler totient function. Since ζ_n is an algebraic integer, $\Phi_n(Z)$ will have integer coefficients. Therefore, it makes sense to view the cyclotomic polynomials in $\mathbb{F}_q[Z]$. From the definition it is easy to see that

$$Z^n - 1 = \prod_{d|n} \Phi_d(Z).$$

When n is prime, we can use this to Diophantinely define the nth cyclotomic polynomial in $\mathbb{F}_q[W, Z]$ as

$$X = \Phi_n \quad \Longleftrightarrow \quad (Z-1)X = Z^n - 1. \tag{26}$$

In the previous section, we constructed a Diophantine model of $\mathbb{N}$, with n being represented by Z^n. This means that (26) gives a Diophantine function $\mathbb{N} \to \mathbb{F}_q[Z]$, mapping n to Φ_n whenever n is prime.

We need the following easy facts about cyclotomic polynomials (some proofs are inspired by [11]):

Proposition 13. *If n is prime to the characteristic p, then $Z^n - 1$ is a squarefree polynomial in $\mathbb{F}_q[Z]$.*

Proof. The derivative of $Z^n - 1$ is nZ^{n-1} with n non-zero in $\mathbb{F}_q$. So $\gcd(Z^n - 1, nZ^{n-1}) = 1$, which implies that $Z^n - 1$ is squarefree. □

Proposition 14. *Let a and b be two distinct integers, both prime to p. Then* $\gcd(\Phi_a, \Phi_b) = 1$ *in $\mathbb{F}_q[Z]$.*

Proof. If Φ_a and Φ_b had a common factor, then $Z^{ab} - 1$, which is a multiple of $\Phi_a\Phi_b$, would not be squarefree. □

Let g and a be coprime integers. In what follows, the notation $\operatorname{ord}(g \bmod a)$ means the order of g seen as an element of the group $(\mathbb{Z}/a\mathbb{Z})^*$. In other words, the smallest positive integer k such that $g^k \equiv 1 \bmod a$.

Proposition 15. *Let a and b be prime, with b not a divisor of $q - 1$. Then*

$$a | \Phi_b(q) \quad \Longleftrightarrow \quad \operatorname{ord}(q \bmod a) = b.$$

Please cite this article as: J. Demeyer, Recursively enumerable sets of polynomials over a finite field, J. Algebra (2006), doi:10.1016/j.jalgebra.2006.09.030

Proof. ($\Rightarrow$) Since b is assumed prime, we know that $\Phi_b(q) = (q^b - 1)/(q - 1)$. It is given that

$$\frac{q^b - 1}{q - 1} \equiv 0 \mod a. \tag{27}$$

We claim that q cannot be congruent to 1 modulo a. Otherwise, we would have

$$0 \equiv \Phi_b(q) = 1 + q + q^2 + \cdots + q^{b-1} \equiv b \mod a.$$

In other words, b would have to be a multiple of a, hence equal to a. By Fermat's Little Theorem and the fact that $q \not\equiv 1 \bmod b$, we have

$$\frac{q^b - 1}{q - 1} \equiv 1 \mod b.$$

This is a contradiction with (27).

Given $q \not\equiv 1 \bmod a$, (27) implies that $q^b \equiv 1 \bmod a$.

($\Leftarrow$) b is prime, so $\operatorname{ord}(q \bmod a) = b$ means

$$q^b \equiv 1 \mod a \quad \text{and} \quad q \not\equiv 1 \mod a.$$

Therefore,

$$\frac{q^b - 1}{q - 1} \equiv 0 \mod a. \qquad \square$$

Proposition 16. *Let a be prime to the characteristic p. Then the irreducible factors of the cyclotomic polynomial Φ_a (seen as an element of $\mathbb{F}_q[Z]$) all have degree equal to* $\operatorname{ord}(q \bmod a)$.

Proof. See [6, Theorem 2.47]. $\square$

Taking the last two propositions together, we get

Corollary 17. *Let q be a power of a prime p. Let a and b be primes with $b \nmid q - 1$. The following are equivalent*:

(1) $a | \Phi_b(q)$.
(2) $a \neq p$ *and* $\operatorname{ord}(q \bmod a) = b$.
(3) $a \neq p$ *and all the irreducible factors of Φ_a over $\mathbb{F}_q$ have degree equal to b.*

Proof. The only thing we still have to prove is that $a \neq p$ whenever $a | \Phi_b(q)$. We know that $a | \Phi_b(q) | q^b - 1$, which implies that $\gcd(a, p) = 1$. $\square$

This can be used to find cyclotomic polynomials with factors of prescribed degree, if that degree is prime and does not divide $q - 1$. This will be one of the main tools in Section 7.

Please cite this article as: J. Demeyer, Recursively enumerable sets of polynomials over a finite field, J. Algebra (2006), doi:10.1016/j.jalgebra.2006.09.030

6. Reducing the problem

6.1. ... to defining the nth polynomial

To prove the Main Theorem, we will use a well-known method to prove the equivalence of recursively enumerable and Diophantine sets (see Section 2 for definitions), which has been successfully applied in [3] and [12]. The idea is to give a Diophantine definition of "X is the nth polynomial in $\mathbb{F}_q[Z]$."

$\mathbb{F}_q[Z]$ is a recursive ring, so we can consider a recursive presentation $\theta : \mathbb{F}_q[Z] \hookrightarrow \mathbb{N}$. The nth polynomial is then the polynomial $\theta^{-1}(n)$.

Theorem 5. *The following are equivalent*:

(1) *Every r.e. subset of* $\mathbb{F}_q[Z]$ *is Diophantine over* $\mathbb{F}_q[W, Z]$.
(2) *For all* $k \geqslant 1$, *every r.e. subset of* $\mathbb{F}_q[Z]^k$ *is Diophantine over* $\mathbb{F}_q[W, Z]$.
(3) *The following relation between* $A \in \mathbb{F}_q[Z]$ *and* $X \in \mathbb{F}_q[Z]$ *is Diophantine over* $\mathbb{F}_q[W, Z]$:

$$\theta(A) = \theta\big(Z^{\theta(X)}\big). \tag{28}$$

Proof. (1 $\Rightarrow$ 2). Take a d such that $p^d > k$, then the polynomial map

$$\begin{aligned} \gamma : \mathbb{F}_q[Z]^k &\to \mathbb{F}_q[Z], \\ (X_1, \ldots, X_k) &\mapsto Z X_1^{p^d} + Z^2 X_2^{p^d} + \cdots + Z^k X_k^{p^d}, \end{aligned}$$

is injective. Take an r.e. set $\mathcal{S} \subseteq \mathbb{F}_q[Z]^k$ and define

$$\mathcal{R} = \gamma(\mathcal{S}) = \big\{ Z X_1^{p^d} + Z^2 X_2^{p^d} + \cdots + Z^k X_k^{p^d} \in \mathbb{F}_q[Z] \;\big|\; (X_1, X_2, \ldots, X_k) \in \mathcal{S} \big\}.$$

This set is r.e., since $\mathcal{S}$ is r.e. We assumed that all r.e. subsets of $\mathbb{F}_q[Z]$ were Diophantine, so $\mathcal{R}$ is Diophantine. Now we can define $\mathcal{S}$ as

$$(X_1, X_2, \ldots, X_k) \in \mathcal{S} \quad \Longleftrightarrow \quad Z X_1^{p^d} + Z^2 X_2^{p^d} + \cdots + Z^k X_k^{p^d} \in \mathcal{R}$$

which is Diophantine.

(2 $\Rightarrow$ 3). Since we have a recursive presentation of $\mathbb{F}_q[Z]$, the relation (28) is recursive as a relation between the integers $\theta(A)$ and $\theta(X)$. By definition of recursive relations over $\mathbb{F}_q[Z]$ (see Section 2), this means that the relation between A and X is recursive. The assumption (for $k = 2$) implies that this relation is Diophantine.

(3 $\Rightarrow$ 1). Take an r.e. subset $\mathcal{S}$ of $\mathbb{F}_q[Z]$. This means that the set $\mathcal{S}^\theta = \{\theta(X) \mid X \in \mathcal{S}\}$ is an r.e. subset of $\mathbb{N}$. By DPRM, $\mathcal{S}^\theta$ is Diophantine over $\mathbb{N}$. Now we can use the model of $\mathbb{N}$ in $\mathbb{F}_q[W, Z]$ to establish that $\mathcal{S}' = \{Z^{\theta(X)} \mid X \in \mathcal{S}\}$ is Diophantine over $\mathbb{F}_q[W, Z]$. For $X \in \mathbb{F}_q[W, Z]$ we have

$$X \in \mathcal{S} \quad \Longleftrightarrow \quad \big(\exists A \in \mathbb{F}_q[W, Z]\big)\, \big(X \in \mathbb{F}_q[Z] \wedge A \in \mathcal{S}' \wedge A = Z^{\theta(X)}\big).$$

Lemma 4 says that "$X \in \mathbb{F}_q[Z]$" is Diophantine and we know by assumption that "$A = Z^{\theta(X)}$" is Diophantine (θ is an injection), so $\mathcal{S}$ is Diophantine. □

Please cite this article as: J. Demeyer, Recursively enumerable sets of polynomials over a finite field, J. Algebra (2006), doi:10.1016/j.jalgebra.2006.09.030

Definition 7. Define $P^{(n)}$ as the polynomial in $\mathbb{F}_q[Z]$ such that $\theta(P^{(n)}) = n$. In other words, $P^{(n)}$ is the polynomial encoded as $n \in \mathbb{N}$, or $P^{(n)}$ is the "nth polynomial." Note that $P^{(n)}$ is only defined when $n \in \operatorname{Im}\theta$.

The preceding theorem reduces the Main Theorem to giving a Diophantine definition of "$\theta(A) = \theta(Z^{\theta(X)})$." But this formula can only be true if A is a power of Z, so it suffices to define "$\theta(Z^n) = \theta(Z^{\theta(X)})$" as a relation between Z^n and X, which is equivalent to "$X = P^{(n)}$."

6.2. … to a bounded universal quantifier

From now on, we use the following notational convention: If we just write $(\exists X)$, with upper case letter, we mean $(\exists X \in \mathbb{F}_q[Z])$. Similarly, we write $(\exists n)$, with lower case letter, instead of $(\exists n \in \mathbb{N})$.

Set $P^{(n)} = \alpha_0^{(n)} Z^d + \alpha_1^{(n)} Z^{d-1} + \cdots + \alpha_d^{(n)}$, where d is the degree of $P^{(n)}$. We also define:

$$\begin{aligned}
Q_{-1}^{(n)} &= 0,\\
Q_0^{(n)} &= \alpha_0^{(n)},\\
Q_1^{(n)} &= \alpha_0^{(n)} Z + \alpha_1^{(n)},\\
&\vdots\\
Q_d^{(n)} &= \alpha_0^{(n)} Z^d + \alpha_1^{(n)} Z^{d-1} + \cdots + \alpha_d^{(n)} = P^{(n)}.
\end{aligned}$$

Clearly, these are only defined when $P^{(n)}$ is defined.

As shown in the previous section, we need to give a Diophantine definition of "$X = P^{(n)}$" to prove the Main Theorem. The following theorem gives a definition, and apart from the bounded universal quantifier $(\forall k)_{\leqslant d}$, it is Diophantine. This quantifier means "for all $k \in \mathbb{N}$ with $k \leqslant d$."

Theorem 6. *Let p_k denote the kth prime number in $\mathbb{N}$, and enumerate $\mathbb{F}_q$ as $\mathbb{F}_q = \{E_1, E_2, \ldots, E_q\}$. Then for $X \in \mathbb{F}_q[Z]$ and $n \in \mathbb{N}$, we have*

$$X = P^{(n)} \tag{29}$$

$$\Updownarrow$$

$$n \in \operatorname{Im}\theta \tag{30}$$

$$\wedge\ (\exists d, e, t)$$

$$d = \deg P^{(n)} \tag{31}$$

$$\wedge\ \beta\big(Q_0^{(n)}, e\big) \wedge \beta\big(Q_1^{(n)}, e\big) \wedge \cdots \wedge \beta\big(Q_d^{(n)}, e\big) \tag{32}$$

$$\wedge\ q^{2e} < p_{t-1} - 1 \tag{33}$$

$$\wedge\ (\exists C)$$

$$0 \equiv C \mod \Phi_{p_{t-1}} \tag{34}$$

$$\wedge\ X \equiv C \mod \Phi_{p_{t+d}} \wedge \beta(X, e) \tag{35}$$

Please cite this article as: J. Demeyer, Recursively enumerable sets of polynomials over a finite field, J. Algebra (2006), doi:10.1016/j.jalgebra.2006.09.030

$$\wedge\, (\forall k)_{\leqslant d}\ (\exists A, Y)$$

$$\left(\alpha_k^{(n)} = E_1 \wedge A = E_1\right) \vee \cdots \vee \left(\alpha_k^{(n)} = E_q \wedge A = E_q\right) \tag{36}$$

$$\wedge\, Y \equiv C \mod \Phi_{p_{t+k-1}} \wedge \beta(Y, e) \tag{37}$$

$$\wedge\, YZ + A \equiv C \mod \Phi_{p_{t+k}}. \tag{38}$$

Remark. Formulas (30)–(33) depend only on the variables d, n, e and t (q is a constant). All these are natural numbers, represented by powers of Z. By DPRM, these formulas are Diophantine over $\mathbb{F}_q[W, Z]$ (see the argument at the end of Section 4.4).

(34), (35), (37) and (38) are Diophantine because the cyclotomic polynomials with prime indices are Diophantinely definable using (26).

Formula (36) simply means "$\alpha_k^{(n)} = A$," but we have to write it like (36) to see that it is Diophantine. For each $1 \leqslant i \leqslant q$, the formula "$\alpha_k^{(n)} = E_i$" depends only on the variables $k, n \in \mathbb{N}$ (every E_i is just a constant), therefore it is Diophantine by DPRM. The language stated in our Main Theorem allows us to define every element of $\mathbb{F}_q$, therefore "$A = E_i$" is also Diophantine.

Proof. Suppose first that $X = P^{(n)}$. Set $d = \deg P^{(n)}$ and take e and t such that (32) and (33) are satisfied. Then use the Chinese Remainder Theorem to find a $C \in \mathbb{F}_q[Z]$ for which

$$\begin{aligned} 0 &\equiv C \mod \Phi_{p_{t-1}}, \\ Q_0^{(n)} &\equiv C \mod \Phi_{p_t}, \\ Q_1^{(n)} &\equiv C \mod \Phi_{p_{t+1}}, \\ &\vdots \\ X = P^{(n)} = Q_d^{(n)} &\equiv C \mod \Phi_{p_{t+d}}. \end{aligned}$$

This gives formulas (34) and (35). Take a k in $\{0, 1, \ldots, d\}$, set $A = \alpha_k^{(n)}$ and $Y = Q_{k-1}^{(n)}$. The choice of C and e give (37). Finally, (38) is true because $Q_{k-1}^{(n)} Z + \alpha_k^{(n)} = Q_k^{(n)}$.

For the other direction ($\Uparrow$), we claim that $Q_k^{(n)} \equiv C \bmod \Phi_{p_{t+k}}$ for $-1 \leqslant k \leqslant d$. We prove it by induction on k. For $k = -1$, the claim is true by (34). Suppose it is true for $k-1$ and let us prove it for k ($0 \leqslant k \leqslant d$). The induction hypothesis, together with (37) and (32) give

$$Y \equiv Q_{k-1}^{(n)} \mod \Phi_{p_{t+k-1}} \wedge \beta(Y, e) \wedge \beta\left(Q_{k-1}^{(n)}, e\right).$$

$\beta(Y, e)$ implies (using (33)) $\deg Y \leqslant q^{2e} < p_{t-1} - 1 \leqslant p_{t+k-1} - 1 = \deg \Phi_{p_{t+k-1}}$, the same bound holds for $\deg Q_{k-1}^{(n)}$. It follows that $Y = Q_{k-1}^{(n)}$. To finish the claim, we use (36) and (38) to get

$$Q_k^{(n)} = Q_{k-1}^{(n)} Z + \alpha_k^{(n)} \equiv YZ + A \equiv C \mod \Phi_{p_{t+k}}.$$

A similar argument, but applied to (35) instead of (37), shows that $X = Q_d^{(n)} = P^{(n)}$. □

Please cite this article as: J. Demeyer, Recursively enumerable sets of polynomials over a finite field, J. Algebra (2006), doi:10.1016/j.jalgebra.2006.09.030

7. Eliminating the bounded universal quantifier

If we take Theorems 5 and 6 together, we see that we can prove our Main Theorem if we can eliminate the bounded universal quantifier (b.u.q.) coming from Theorem 6.

Consider the formula

$$(\forall k)_{\leqslant y}\ (\exists X_1, \ldots, X_m)\ \Delta\big(Z^y, Z^k, F_1, \ldots, F_n, X_1, \ldots, X_m\big) = 0$$

where $F_1, \ldots, F_n$ are free (unbounded) variables and Δ is a polynomial with coefficients in $\mathbb{F}_q[Z]$. This is the general form of a formula with a b.u.q. followed by something Diophantine.

If we set $d = \deg \Delta$ (total degree), we get constants d, n, m as a function of Δ. First we need a small lemma to write this formula in a special form (but still with a b.u.q.). It is then in this form that we will eliminate the b.u.q. to get an equivalent formula with only existential quantifiers.

Lemma 7.

$$(\forall k)_{\leqslant y}\ (\exists X_1, \ldots, X_m)\ \Delta\big(Z^y, Z^k, F_1, \ldots, F_n, X_1, \ldots, X_m\big) = 0 \tag{39}$$

$$\Updownarrow$$

$$(\exists u, e, t)$$

$$\beta(F_1, e) \wedge \cdots \wedge \beta(F_n, e) \tag{40}$$

$$\wedge\ d \cdot \max\big\{y, q^{2e}, q^{2u}\big\} \leqslant t \tag{41}$$

$$\wedge\ (\forall k)_{\leqslant y}\ (\exists X_1, \ldots, X_m)_{\in \mathcal{B}_u}$$

$$\Delta\big(Z^y, Z^k, F_1, \ldots, F_n, X_1, \ldots, X_m\big) = 0. \tag{42}$$

Proof. Assuming (39), there exist $X_1^{(0)}, \ldots, X_m^{(0)}, \ldots, X_1^{(y)}, \ldots, X_m^{(y)}$ such that

$$\Delta\big(Z^y, Z^k, F_1, \ldots, F_n, X_1^{(k)}, \ldots X_m^{(k)}\big) = 0 \quad (0 \leqslant k \leqslant y).$$

We know from Corollary 12 that there exists a $u \in \mathbb{N}$ such that

$$\big\{X_1^{(0)}, \ldots, X_m^{(0)}, X_1^{(1)}, \ldots, X_m^{(1)}, \ldots, X_1^{(y)}, \ldots, X_m^{(y)}\big\} \subseteq \mathcal{B}_u.$$

We choose e such that (40) holds, and t big enough to satisfy (41).

The other implication is trivial. □

In the next theorem, we will eliminate the b.u.q. from formula (42). Instead of trying to prove that (42) is Diophantine by itself, we will prove that "(40) ∧ (41) ∧ (42)" is Diophantine. In Theorem 8 below, we will give a Diophantine formula, and show that it is equivalent to (42), assuming that (40) and (41) are true. If either (40) or (41) is false, then "(40) ∧ (41) ∧ (42)" is false anyway, so then it does not matter whether (42) is still equivalent to the Diophantine formula.

Please cite this article as: J. Demeyer, Recursively enumerable sets of polynomials over a finite field, J. Algebra (2006), doi:10.1016/j.jalgebra.2006.09.030

Theorem 8. *Let $F_1, \ldots, F_n \in \mathbb{F}_q[Z]$ and $y, u, e, t \in \mathbb{N}$. Assume* (40) *and* (41) *are satisfied. Let $b_0, b_1, \ldots, b_y$ be distinct primes, all greater than t, and none of them a divisor of $q-1$. Choose a_k $(0 \leqslant k \leqslant y)$ as a prime factor of $\Phi_{b_k}(q)$. Then*

$$(\forall k)_{\leqslant y}\ (\exists X_1, \ldots, X_m)_{\in \mathcal{B}_u}\ \Delta\big(Z^y, Z^k, F_1, \ldots, F_n, X_1, \ldots, X_m\big) = 0 \tag{43}$$

$$\Updownarrow$$

$$(\exists c)\ (\exists A_1, \ldots, A_m)\ (\exists P)$$

$$c \equiv k \mod a_k \quad (0 \leqslant k \leqslant y) \tag{44}$$

$$\wedge\ \Phi_{a_0}\Phi_{a_1}\cdots\Phi_{a_y} \mid P \mid \frac{Z^{a_0 a_1 \ldots a_y} - 1}{Z - 1} \tag{45}$$

$$\wedge\ P \Big| \prod_{J \in \mathcal{B}_u} (A_i - J) \quad (1 \leqslant i \leqslant m) \tag{46}$$

$$\wedge\ \Delta\big(Z^y, Z^c, F_1, \ldots, F_n, A_1, \ldots, A_m\big) \equiv 0 \mod P. \tag{47}$$

Proof. First of all, the primes a_k are all distinct (this follows from Proposition 14 or Corollary 17).

Suppose we have

$$\Delta\big(Z^y, Z^k, F_1, \ldots, F_n, X_1^{(k)}, \ldots, X_m^{(k)}\big) = 0 \quad \text{with } X_i^{(k)} \in \mathcal{B}_u\ (0 \leqslant k \leqslant y). \tag{48}$$

Use the Chinese Remainder Theorem to get a c satisfying (44). This implies that $Z^c \equiv Z^k \bmod Z^{a_k} - 1$, in particular $Z^c \equiv Z^k \bmod \Phi_{a_k}$.

Now we apply the Chinese Remainder Theorem again to choose $A_1, \ldots, A_m \in \mathbb{F}_q[Z]$ such that

$$A_i \equiv X_i^{(k)} \mod \Phi_{a_k} \quad (1 \leqslant i \leqslant m,\ 0 \leqslant k \leqslant y). \tag{49}$$

We can do this, because the moduli Φ_{a_k} are coprime by Proposition 14.

Using (48), we get

$$\begin{aligned}&\Delta\big(Z^y, Z^c, F_1, \ldots, F_n, A_1, \ldots, A_m\big)\\ &\quad\equiv \Delta\big(Z^y, Z^k, F_1, \ldots, F_n, X_1^{(k)}, \ldots, X_m^{(k)}\big) \equiv 0 \mod \Phi_{a_k}.\end{aligned}$$

Since this holds for all k, this implies (47), if we set $P = \Phi_{a_0}\Phi_{a_1}\cdots\Phi_{a_y}$ (this way (45) is also satisfied).

Using the fact that $X_i^{(k)} \in \mathcal{B}_u$, it follows from (49) that

$$\prod_{J \in \mathcal{B}_u} (A_i - J) \equiv 0 \mod \Phi_{a_k} \quad (1 \leqslant i \leqslant m,\ 0 \leqslant k \leqslant y).$$

This immediately implies (46).

Please cite this article as: J. Demeyer, Recursively enumerable sets of polynomials over a finite field, J. Algebra (2006), doi:10.1016/j.jalgebra.2006.09.030

For the other direction, we assume the bottom part of the theorem holds. Taking a k less than or equal to y, we need to find $X_1^{(k)}, \ldots, X_m^{(k)} \in \mathcal{B}_u$ for which (43) is satisfied. (45) and (46) give us

$$\Phi_{a_k}|P| \prod_{J \in \mathcal{B}_u} (A_i - J) \quad (1 \leqslant i \leqslant m,\ 0 \leqslant k \leqslant y).$$

Let Ψ_{a_k} be any irreducible factor of Φ_{a_k}. Corollary 17 tells us that $\deg \Psi_{a_k} = \operatorname{ord}(q \bmod a_k) = b_k$.

Ψ_{a_k} is irreducible (and prime because of unique factorization), so if it divides a product, it divides one of the factors, say $\Psi_{a_k}|A_i - X_i^{(k)}$, with $X_i^{(k)} \in \mathcal{B}_u$. Written otherwise, this becomes

$$A_i \equiv X_i^{(k)} \mod \Psi_{a_k} \quad (1 \leqslant i \leqslant m,\ 0 \leqslant k \leqslant y).$$

From (44) it follows that $Z^c \equiv Z^k \bmod \Psi_{a_k}$. All this gives

$$\begin{aligned} &\Delta\big(Z^y, Z^k, F_1, \ldots, F_n, X_1^{(k)}, \ldots, X_m^{(k)}\big) \\ &\quad \equiv \Delta\big(Z^y, Z^c, F_1, \ldots, F_n, A_1, \ldots, A_m\big) \equiv 0 \mod \Psi_{a_k}. \end{aligned}$$

If we can prove that the degree of the left-hand side is less than the degree of Ψ_{a_k}, we are done. For this we will use the assumptions of the theorem (recall that d is the total degree of Δ),

$$\begin{aligned} &\deg \Delta\big(Z^y, Z^k, F_1, \ldots, F_n, X_1^{(k)}, \ldots, X_m^{(k)}\big) \\ &\quad \leqslant d \cdot \max\big\{\deg Z^y, \deg Z^k, \deg F_1, \ldots, \deg F_n, \deg X_1^{(k)}, \ldots, \deg X_m^{(k)}\big\} \\ &\quad \leqslant d \cdot \max\big\{y, q^{2e}, q^{2u}\big\} \leqslant t \\ &\quad < b_k = \deg \Psi_{a_k}. \qquad \square \end{aligned}$$

This theorem does indeed reduce the original formula with a b.u.q. to one with only existential quantifiers. However, it is far from clear that all the formulas used are Diophantine, in particular (45) and (46) seem problematic. We will prove that even these are Diophantine (see Sections 7.2 and 7.3). For the other formulas, it is easy to see that they are Diophantine, we will discuss this in more detail in Section 7.4.

To prove that (46) is Diophantine, we will need the second variable W. That is the only place in this paper where W is needed. Therefore, if one could prove that (46) is Diophantine over $\mathbb{F}_q[Z]$ (as opposed to $\mathbb{F}_q[W, Z]$), then it would follow that r.e. sets in $\mathbb{F}_q[Z]$ are Diophantine over $\mathbb{F}_q[Z]$.

7.1. Product rings

In this interlude we study Diophantine equations over a product ring (all rings we consider are commutative with 1) $\mathcal{R} = \mathcal{R}_1 \times \mathcal{R}_2 \times \cdots \times \mathcal{R}_f$. Such rings arise naturally by the Chinese Remainder Theorem when working in a ring modulo a (non-primary) ideal. We will need this in the next two sections.

The following proposition more or less says that a Diophantine equation has a solution in a product ring if and only if it has a solution in each of the rings separately.

Please cite this article as: J. Demeyer, Recursively enumerable sets of polynomials over a finite field, J. Algebra (2006), doi:10.1016/j.jalgebra.2006.09.030

Proposition 18. *Let $\mathcal{R}_1, \mathcal{R}_2, \ldots, \mathcal{R}_f$ be rings, and set $\mathcal{R} = \mathcal{R}_1 \times \mathcal{R}_2 \times \cdots \times \mathcal{R}_f$, with the natural projection maps $\pi_j : \mathcal{R} \to \mathcal{R}_j$ $(1 \leqslant j \leqslant f)$. Let $F_1, \ldots, F_n$ be elements of $\mathcal{R}$, and Δ a polynomial over $\mathbb{Z}$ in $n+m$ variables. Consider the Diophantine equation*

$$\Delta(F_1, \ldots, F_n, X_1, \ldots, X_m) = 0. \tag{50}$$

This equation has a solution $(X_1, \ldots, X_m) \in \mathcal{R}^m$ if and only if the system

$$\begin{cases} \Delta(\pi_1(F_1), \ldots, \pi_1(F_n), X_1^{(1)}, \ldots, X_m^{(1)}) = 0 \quad (\text{in } \mathcal{R}_1), \\ \quad \vdots \\ \Delta(\pi_f(F_1), \ldots, \pi_f(F_n), X_1^{(f)}, \ldots, X_m^{(f)}) = 0 \quad (\text{in } \mathcal{R}_f) \end{cases} \tag{51}$$

has a solution $(X_i^{(j)})_{1 \leqslant i \leqslant m,\ 1 \leqslant j \leqslant f}$ where $X_i^{(j)} \in \mathcal{R}_j$.

Proof. One direction is trivial: if (50) holds, then we simply take $X_i^{(j)} = \pi_j(X_i)$. Equation (50) implies $\pi_j(\Delta(F_1, \ldots, F_n, X_1, \ldots, X_m)) = 0$ for all $j = 1, \ldots, f$. The projections π_j are ring morphisms, so all equations in the system (51) will be satisfied.

Conversely, assume we have a solution for (51). Set

$$X_i = \left(X_i^{(1)}, X_i^{(2)}, \ldots, X_i^{(f)}\right) \in \mathcal{R}_1 \times \mathcal{R}_2 \times \cdots \times \mathcal{R}_f = \mathcal{R}.$$

(50) is equivalent to

$$\pi_j\left(\Delta(F_1, \ldots, F_n, X_1, \ldots, X_m)\right) = 0 \quad \text{for all } j = 1, \ldots, f.$$

The projections are ring morphisms, so this is equivalent to

$$\Delta\left(\pi_j(F_1), \ldots, \pi_j(F_n), \pi_j(X_1), \ldots, \pi_j(X_m)\right) = 0 \quad \text{for all } j = 1, \ldots, f.$$

But we know the latter is true because $\pi_j(X_i) = X_i^{(j)}$. □

In this proposition, "$\Delta(F_1, \ldots, F_n, X_1, \ldots, X_m) = 0$" is a so-called atomic formula in the language of rings $\mathcal{L}_R = \{+, \cdot, 0, 1\}$. The proposition still holds if we allow conjunctions ($\wedge$). But adding disjunctions ($\vee$) or inequations ($\neq$) breaks it. Counterexamples:

- "$(2X = 1) \vee (3X = 1)$" has solutions in $\mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/3\mathbb{Z}$, but not in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$.
- "$(2X \neq 0)$" has a solution in $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$, but not in $\mathbb{Z}/2\mathbb{Z}$.

If we apply Proposition 18 to the Chinese Remainder Theorem, we get:

Corollary 19. *Let $\mathcal{R}$ be a ring, let $\mathcal{I}_1, \ldots, \mathcal{I}_f$ be pairwise coprime ideals (i.e. $\mathcal{I}_i + \mathcal{I}_j = \mathcal{R}$ whenever $i \neq j$), and set $\mathcal{I} = \prod_{j=1}^{f} \mathcal{I}_j$. Let $F_1, \ldots, F_n$ be elements of $\mathcal{R}$ (or $\mathcal{R}/\mathcal{I}$), and Δ a polynomial over $\mathbb{Z}$ in $n+m$ variables. Consider the equation*

$$\Delta(F_1, \ldots, F_n, X_1, \ldots, X_m) \equiv 0 \mod \mathcal{I}. \tag{52}$$

Please cite this article as: J. Demeyer, Recursively enumerable sets of polynomials over a finite field, J. Algebra (2006), doi:10.1016/j.jalgebra.2006.09.030

This has a solution if and only if the following system has a solution:

$$\begin{cases} \Delta(F_1, \ldots, F_n, X_1^{(1)}, \ldots, X_m^{(1)}) \equiv 0 \mod \mathcal{I}_1, \\ \quad \vdots \\ \Delta(F_1, \ldots, F_n, X_1^{(f)}, \ldots, X_m^{(f)}) \equiv 0 \mod \mathcal{I}_f. \end{cases} \tag{53}$$

7.2. Defining (45)

We can now tackle formula (45) from Theorem 8. As in that theorem, let $b_0, b_1, \ldots, b_y$ be distinct primes and a_k $(0 \leqslant k \leqslant y)$ a prime factor of $\Phi_{b_k}(q)$. Set

$$r = (q-1)\Phi_{b_0}(q)\Phi_{b_1}(q)\cdots\Phi_{b_y}(q). \tag{54}$$

Lemma 9. *Let $b_0, b_1, \ldots, b_y$ be distinct primes and r as in* (54)*. For all $0 \leqslant i < j \leqslant y$, $q^{b_i b_j} - 1$ is not a divisor of r.*

Proof. To find a contradiction, we assume

$$q^{b_i b_j} - 1 \Big| (q-1) \prod_{k=0}^{y} \Phi_{b_k}(q).$$

Dividing both sides by $(q-1)\Phi_{b_i}(q)\Phi_{b_j}(q)$ gives

$$\Phi_{b_i b_j}(q) \Big| \prod_{k \neq i, k \neq j} \Phi_{b_k}(q).$$

Let a be any prime dividing $\Phi_{b_i b_j}(q)$. Then a has to divide $\Phi_{b_k}(q)$ for a certain k different from i and j. Since b_k is prime, this implies that $\operatorname{ord}(q \bmod a) = b_k$ by Proposition 15. But $a | \Phi_{b_i b_j}(q)$ implies that $q^{b_i b_j} \equiv 1 \bmod a$. This is a contradiction because $b_i b_j$ would have to be a multiple of b_k. □

Theorem 10. *Let a_k, b_k $(0 \leqslant k \leqslant y)$ and r be chosen as above. Then*

$$\Phi_{a_0}\Phi_{a_1}\cdots\Phi_{a_y} | P | \frac{Z^{a_0 a_1 \ldots a_y} - 1}{Z - 1} \tag{55}$$

$$\Updownarrow$$

$$(\exists Q, G, H, M)$$

$$(Z-1)PQ = \left(Z^{a_0 a_1 \ldots a_y} - 1\right) \tag{56}$$

$$\wedge\, GH \equiv 1 \mod Q \tag{57}$$

$$\wedge \left(G^r - 1\right) M \equiv 1 \mod Q. \tag{58}$$

Please cite this article as: J. Demeyer, Recursively enumerable sets of polynomials over a finite field, J. Algebra (2006), doi:10.1016/j.jalgebra.2006.09.030

Proof. Assume (55). To get (56), set

$$Q = \frac{Z^{a_0 a_1 \ldots a_y} - 1}{(Z-1)P}$$

which is a polynomial by assumption. It follows from the theory of cyclotomic polynomials (see Section 5) that

$$Z^{a_0 a_1 \ldots a_y} - 1 = \prod_{d | a_0 a_1 \ldots a_y} \Phi_d = \underbrace{(Z-1)}_{\Phi_1} \underbrace{\Phi_{a_0} \Phi_{a_1} \cdots \Phi_{a_y}}_{\substack{\Phi_d \text{ with } d | a_0 a_1 \ldots a_y, \\ d \text{ prime}}} \underbrace{\Phi_{a_0 a_1} \Phi_{a_0 a_2} \cdots \Phi_{a_0 a_1 \ldots a_y}}_{\substack{\Phi_d \text{ with } d | a_0 a_1 \ldots a_y, \\ d \text{ having at least 2 factors}}}.$$

Since $\Phi_{a_0} \Phi_{a_1} \cdots \Phi_{a_y} | P$, this implies that

$$Q \Big| \prod_{\substack{d | a_0 a_1 \ldots a_y, \\ d \text{ has } \geqslant 2 \text{ factors}}} \Phi_d. \tag{59}$$

We will apply Corollary 19 on the irreducible factors of Q to prove (57) and (58). So, for each irreducible factor Ψ of Q, we need to find G, H and M such that (57) and (58) are satisfied modulo Ψ. Note that G, H and M may depend on Ψ.

By (59), an irreducible factor of Q will be a divisor of a particular Φ_d. We denote this factor by Ψ_d. We know that d has at least 2 prime factors, say a_i and a_j $(i \neq j)$. By Proposition 16, the degree of Ψ_d is equal to $\operatorname{ord}(q \bmod d)$, so working modulo Ψ_d is the same as working in the finite field $\mathbb{F}_{q^{\operatorname{ord}(q \bmod d)}}$. From the definition of ord it is clear that

$$a_i | d \quad \Longrightarrow \quad \operatorname{ord}(q \bmod a_i) | \operatorname{ord}(q \bmod d) \quad \Longrightarrow \quad b_i | \operatorname{ord}(q \bmod d).$$

Analogously, we have $b_j | \operatorname{ord}(q \bmod d)$. Both b_i and b_j are prime, so $b_i b_j$ divides $\operatorname{ord}(q \bmod d)$. Let G be a generator of the multiplicative group of the subfield $\mathbb{F}_{q^{b_i b_j}} \subseteq \mathbb{F}_{q^{\operatorname{ord}(q \bmod d)}}$. Then G has an inverse H. By Lemma 9, r is not a multiple of the order of this group, so $G^r \neq 1$, hence $G^r - 1$ has an inverse M. This proves (57) and (58) modulo Ψ_d.

For the converse, it follows from (56) that

$$\Phi_{a_0} \Phi_{a_1} \cdots \Phi_{a_y} \Big| \frac{Z^{a_0 a_1 \ldots a_y} - 1}{Z - 1} = PQ.$$

We are done if we can prove that $\gcd(\Phi_{a_k}, Q) = 1$ for all k. Suppose this is not the case, and let Ψ_{a_k} be a common irreducible factor of Φ_{a_k} and Q. Then (57) implies that $G \not\equiv 0 \bmod \Psi_{a_k}$. But the order of $(\mathbb{F}_q[Z]/\Psi_{a_k})^*$ is equal to $q^{\deg \Psi_{a_k}} - 1 = q^{b_k} - 1 = (q-1)\Phi_{b_k}(q)$, which divides r. Therefore, $G^r \equiv 1 \bmod \Psi_{a_k}$, in contradiction to (58). □

7.3. Defining (46)

In this section we will prove that formula (46) from Theorem 8 is Diophantine. We only need to define it in the case that (45) holds. This is the point where we need to use the variable W.

Please cite this article as: J. Demeyer, Recursively enumerable sets of polynomials over a finite field, J. Algebra (2006), doi:10.1016/j.jalgebra.2006.09.030

Theorem 11. *Let P be a polynomial in $\mathbb{F}_q[Z]$ dividing $Z^{a_0a_1\ldots a_y}-1$, and let $A\in\mathbb{F}_q[Z]$. Then*

$$P\Big|\prod_{J\in\mathcal{B}_u}(A-J) \tag{60}$$

$$\Updownarrow$$

$$(\exists s,w)$$

$$s \text{ is prime} \wedge s>q^{2u} \wedge s\nmid q-1 \wedge s\nmid \varphi(a_0a_1\ldots a_y) \tag{61}$$

$$\wedge\, w \text{ is prime} \wedge w|\Phi_s(q) \tag{62}$$

$$\wedge\,\big(\exists B\in\mathbb{F}_q[W,Z]\big)\,\big(\exists M^{(1)},M^{(2)},M^{(3)}\in\mathbb{F}_q[W,Z]\big)$$

$$B^2M^{(1)}\equiv\big(W^{q^{2u}}-W^{q^u}\big)B \mod P(Z) \tag{63}$$

$$\wedge\,\Phi_w(W)M^{(2)}\equiv B^{q^s}-B \mod P(Z) \tag{64}$$

$$\wedge\,(W-Z)M^{(3)}\equiv A-B \mod P(Z). \tag{65}$$

We claim that it suffices to prove this theorem for P irreducible. Indeed, assume P factors as

$$P=\prod_{j=1}^{f}P_j \quad (P_j \text{ irreducible}).$$

All these factors will be distinct, since P divides the squarefree polynomial $Z^{a_0a_1\ldots a_y}-1$.

It is clear that (60) holds for P if and only if it holds for all P_j. In the bottom part, s and w do not depend on P, and the other equations all work modulo P, so we can apply Corollary 19. That version of the Chinese Remainder Theorem works because the P_i are distinct irreducible polynomials in $\mathbb{F}_q[Z]$. This means that $(P_i)+(P_j)=(1)$ whenever $i\neq j$.

We will now do the proof of Theorem 11 for P irreducible. P is a divisor of $Z^{a_0a_1\ldots a_y}-1$, so $P=\Psi_d(Z)$, where Ψ_d is an irreducible factor of Φ_d for a certain $d|a_0a_1\ldots a_y$. We can interpret working modulo $P=\Psi_d(Z)$ as working in the ring $\mathbb{F}_q[W,Z]/P\cong\mathbb{F}_{q^h}[W]$, where $h=\deg\Psi_d=\operatorname{ord}(q \bmod d)$ according to Proposition 16 (neither d nor h have to be prime for this).

This means that we have to prove

Theorem 12. *Let Ψ_d be an irreducible factor of Φ_d, with $d|a_0a_1\ldots a_y$. Set $h=\deg\Psi_d=\operatorname{ord}(q \bmod d)$. Let $\overline{Z}$ denote the reduction of Z modulo $\Psi_d(Z)$, and $\overline{\mathcal{B}_u}$ the reduction of the set $\mathcal{B}_u\subset\mathbb{F}_q[Z]$ modulo $\Psi_d(Z)$. Then for $A\in\mathbb{F}_{q^h}$ we have*

$$A\in\overline{\mathcal{B}_u} \tag{66}$$

$$\Updownarrow$$

$$(\exists s,w)$$

$$s \text{ is prime} \wedge s>q^{2u} \wedge s\nmid q-1 \wedge s\nmid \varphi(a_0a_1\ldots a_y) \tag{67}$$

$$\wedge\, w \text{ is prime} \wedge w|\Phi_s(q) \tag{68}$$

$$\wedge\,\big(\exists B\in\mathbb{F}_{q^h}[W]\big)$$

$$B^2\Big|\big(W^{q^{2u}}-W^{q^u}\big)B \tag{69}$$

Please cite this article as: J. Demeyer, Recursively enumerable sets of polynomials over a finite field, J. Algebra (2006), doi:10.1016/j.jalgebra.2006.09.030

$$\wedge\, B^{q^s} \equiv B \mod \Phi_w(W) \tag{70}$$

$$\wedge\, A \equiv B \mod W - \overline{Z}. \tag{71}$$

Proof. If (66) holds, then by definition of $\mathcal{B}_u$ (see Section 4.6), there exists a polynomial $X(\xi) \in \mathbb{F}_q[\xi]$ (note: $\mathbb{F}_q[\xi]$, not $\mathbb{F}_{q^h}[\xi]$) such that

$$A = X(\overline{Z}) \tag{72}$$

$$\wedge\, X(\xi)^2 \big| \big(\xi^{q^{2u}} - \xi^{q^u}\big) X(\xi) \quad \big(\text{in } \mathbb{F}_q[\xi]\big). \tag{73}$$

Substituting W for ξ in (73) gives

$$X(W)^2 \big| \big(W^{q^{2u}} - W^{q^u}\big) X(W).$$

We get (69) if we set

$$B = X(W). \tag{74}$$

Take s and w satisfying (67) and (68). By Corollary 17, $\Phi_w(W)$ factors in polynomials of degree s, so

$$\mathbb{F}_q[W]/\Phi_w(W) \cong \mathbb{F}_{q^s} \times \cdots \times \mathbb{F}_{q^s}.$$

Therefore,

$$X(W)^{q^s} \equiv X(W) \mod \Phi_w(W).$$

Since $B = X(W)$, we have (70).

Reducing (74) modulo $W - \overline{Z}$ gives

$$B \equiv X(\overline{Z}) \mod W - \overline{Z}.$$

Since $A = X(\overline{Z})$, we get (71).

Conversely, assume (67) to (71) hold. From formula (69) follows that $\deg B \leqslant q^{2u}$, hence there exist $B_0, B_1, \ldots, B_{q^{2u}} \in \mathbb{F}_{q^h}$ such that

$$B = B_0 + B_1 W + B_2 W + \cdots + B_{q^{2u}} W^{q^{2u}}. \tag{75}$$

Recall $h = \operatorname{ord}(q \bmod d)$, implying that $h | \varphi(d) | \varphi(a_0 a_1 \ldots a_y)$. Since s is prime and $s \nmid \varphi(a_0 a_1 \ldots a_y)$, this means that $\gcd(h, s) = 1$. Now

$$\operatorname{ord}\big(q^h \bmod w\big) = \frac{\operatorname{ord}(q \bmod w)}{\gcd(h, \operatorname{ord}(q \bmod w))} = \frac{s}{\gcd(h, s)} = s = \operatorname{ord}(q \bmod w).$$

This means that the irreducible factors of $\Phi_w(W)$ over $\mathbb{F}_{q^h}$ have degree s, so they must be the same as the irreducible factors of $\Phi_w(W)$ over $\mathbb{F}_q$. Let $\Psi_w(W)$ be such a factor. Note that $\mathbb{F}_q[W]/\Psi_w(W) \cong \mathbb{F}_{q^s}$, therefore $W^{q^s} \equiv W \bmod \Psi_w(W)$.

Please cite this article as: J. Demeyer, Recursively enumerable sets of polynomials over a finite field, J. Algebra (2006), doi:10.1016/j.jalgebra.2006.09.030

Now reduce Eq. (75) modulo $\Psi_w(W)$:

$$B \equiv B_0 + B_1 W + B_2 W^2 + \cdots + B_{q^{2u}} W^{q^{2u}} \mod \Psi_w(W). \tag{76}$$

We raise both sides to the power q^s, taking into account $B^{q^s} \equiv B \mod \Psi_w(W)$ by (70) and $W^{q^s} \equiv W \mod \Psi_w(W)$:

$$B \equiv B_0^{q^s} + B_1^{q^s} W + B_2^{q^s} W^2 + \cdots + B_{q^{2u}}^{q^s} W^{q^{2u}} \mod \Psi_w(W). \tag{77}$$

The right-hand sides of (76) and (77) are both polynomials in $\mathbb{F}_{q^h}[W]$ of degree at most $q^{2u} < s$. They are congruent modulo $\Psi_w(W)$, which has degree s, so they must be equal, hence $B_i^{q^s} = B_i$ for all i. The B_i are the coefficients of B, a priori these were chosen in $\mathbb{F}_{q^h}$. However, we now see that they are also in $\mathbb{F}_{q^s}$. Since $\gcd(h, s) = 1$, it follows that $B_i \in \mathbb{F}_{q^h} \cap \mathbb{F}_{q^s} = \mathbb{F}_q$.

Going back to (75), all this means that there exists a polynomial $X(\xi) \in \mathbb{F}_q[\xi]$ (note: $\mathbb{F}_q[\xi]$, not $\mathbb{F}_{q^h}[\xi]$) such that

$$B = X(W).$$

Together with (69) this gives

$$X(W)^2 \big| \big(W^{q^{2u}} - W^{q^u}\big) X(W).$$

This condition states exactly that $X \in \mathcal{B}_u$. Finally, observe that

$$A \equiv B \equiv X(W) \equiv X(\overline{Z}) \mod W - \overline{Z}.$$

Since A and $X(\overline{Z})$ are constants (elements of $\mathbb{F}_{q^h}$), this actually means that A is equal to $X(\overline{Z}) \in \overline{\mathcal{B}_u}$. □

7.4. Putting everything together

Putting Lemma 7 and Theorems 8, 10 and 11 together, we get the following equivalence:

$$\begin{aligned}
&(\forall k)_{\leqslant y}\ (\exists X_1, \ldots, X_m)\ \Delta\big(Z^y, Z^k, F_1, \ldots, F_n, X_1, \ldots, X_m\big) = 0 \\
&\qquad\qquad \Updownarrow \\
&\qquad (\exists u, e, t) \\
&\qquad\qquad \beta(F_1, e) \wedge \cdots \wedge \beta(F_n, e) \\
&\qquad\qquad \wedge\, d \cdot \max\big\{y, q^{2e}, q^{2u}\big\} \leqslant t \\
&\wedge\ (\exists \bar{b} \in \mathbb{N})\ (\exists \bar{a} \in \mathbb{N}) \\
&\qquad\qquad \bar{b} \text{ is a product of } y+1 \text{ primes } b_0, b_1, \ldots, b_y \text{ with} \\
&\qquad\qquad\qquad t < b_0 < b_1 < \cdots < b_y \text{ and } b_k \nmid q - 1 \text{ for all } k \\
&\qquad\qquad \wedge\, \bar{a} \text{ is a product of } y+1 \text{ primes } a_0 < a_1 < \cdots < a_y, \\
&\qquad\qquad\qquad \text{with } a_k \text{ a divisor of } \Phi_{b_k}(q)
\end{aligned}$$

Please cite this article as: J. Demeyer, Recursively enumerable sets of polynomials over a finite field, J. Algebra (2006), doi:10.1016/j.jalgebra.2006.09.030

$$
\begin{aligned}
&\wedge (\exists c)\ (\exists A_1, \ldots, A_m)\ (\exists P) \\
&\qquad c \equiv k \mod a_k \quad (0 \leqslant k \leqslant y) \\
&\qquad \wedge\ \Delta\big(Z^y, Z^c, F_1, \ldots, F_n, A_1, \ldots, A_m\big) \equiv 0 \mod P \\
&\wedge (\exists r)\ (\exists Q, G, H, M) \\
&\qquad r = (q-1)\Phi_{b_0}(q)\Phi_{b_1}(q)\cdots\Phi_{b_y}(q) \\
&\qquad \wedge\ (Z-1)PQ = \big(Z^{\bar{a}} - 1\big) \\
&\qquad \wedge\ GH \equiv 1 \mod Q \\
&\qquad \wedge\ \big(G^r - 1\big)M \equiv 1 \mod Q \\
&\quad \wedge (\exists s, w) \\
&\qquad s \text{ is prime} \wedge s > q^{2u} \wedge s \nmid q-1 \wedge s \nmid \varphi(a_0 a_1 \ldots a_y) \\
&\qquad \wedge\ w \text{ is prime} \wedge w | \Phi_s(q) \\
&\wedge \bigwedge_{i=1}^{m} \big(\exists B_i \in \mathbb{F}_q[W, Z]\big) \\
&\qquad \big(W^{q^{2u}} - W^{q^u}\big)B_i \equiv 0 \mod \big(P, B_i^2\big) \\
&\qquad \wedge\ B_i^{q^s} \equiv B_i \mod \big(P, \Phi_w(W)\big) \\
&\qquad \wedge\ A_i \equiv B_i \mod (P, W - Z).
\end{aligned}
$$

In this formula, d, m and n are constants depending on the given Δ. Then we have constants p and q coming from the ring we work in. The variables $F_1, \ldots, F_n$ and y (represented by Z^y) occur free (unbounded).

b_0 through b_y are not really variables; b_i is just a notation for a recursive function applied on the variable $\bar{b}$, returning the ith smallest prime factor of $\bar{b}$. The formula saying that "$\bar{b}$ is a product ..." is a relation between the variables $\bar{b}$, y and t. Similarly, $a_0, \ldots, a_y$ are not variables, but $\bar{a}$ is.

There are several formulas whose variables run only in the natural numbers. These variables are represented by powers of Z and have to be interpreted as explained in Section 4.4. Therefore, these formulas are Diophantine. Special attention has to be paid to the formula "$c \equiv k \mod a_k$ for all $0 \leqslant k \leqslant y$." This must be seen as one formula, in the variables c, y and $\bar{a}$. We cannot write this down as a system of y formulas, because y is not constant.

Finally, the last three formulas correspond to (63)–(65), but we have rewritten them as a congruence modulo an ideal generated by two polynomials.

All the other formulas are easily seen to be Diophantine. Also note that the only quantifiers appearing are existential. Therefore, the whole formula, which is equivalent to $(\forall k)_{\leqslant y}\ (\exists X_1, \ldots, X_m)\ \Delta(Z^y, Z^k, F_1, \ldots, F_n, X_1, \ldots, X_m) = 0$, is Diophantine. Looking back at Theorems 5 and 6, we may conclude that we have proven the Main Theorem.

Acknowledgments

The author thanks Joseph Flenner for reading this paper very carefully and pointing out many mistakes and shortcomings. Thanks also go to Bjorn Poonen for the discussions we had, espe-

Please cite this article as: J. Demeyer, Recursively enumerable sets of polynomials over a finite field, J. Algebra (2006), doi:10.1016/j.jalgebra.2006.09.030

cially about Section 7.3. Finally, many thanks to Jan Van Geel and Karim Zahidi for helping me throughout with this paper.

References

[1] M. Davis, Hilbert's tenth problem is unsolvable, Amer. Math. Monthly 80 (1973) 233–269.
[2] M. Davis, H. Putnam, Diophantine sets over polynomial rings, Illinois J. Math. 7 (1963) 251–256.
[3] J. Denef, Diophantine sets over $\mathbb{Z}[T]$, Proc. Amer. Math. Soc. 69 (1978) 148–150.
[4] J. Denef, The Diophantine problem for polynomial rings of positive characteristic, in: Logic Colloquium, 1978, North-Holland, 1979, pp. 131–145.
[5] A. Fröhlich, C. Shepherdson, Effective procedures in field theory, Philos. Trans. R. Soc. Lond. Ser. A Math. Phys. Eng. Sci. 248 (1956) 407–432.
[6] R. Lidl, H. Niederreiter, Introduction to Finite Fields and Their Applications, Cambridge Univ. Press, 1988.
[7] Y. Matiyasevič, Enumerable sets are Diophantine, Soviet Math. Dokl. 11 (1970) 354–358.
[8] T. Pheidas, K. Zahidi, Undecidability of existential theories of rings and fields: A survey, in: Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry, Ghent, 1999, in: Contemp. Math., vol. 270, 2000, pp. 49–105.
[9] B. Poonen, Hilbert's tenth problem over rings of number-theoretic interest, Arizona Winter School 2003 notes (at the time of writing, available from the author's web site), 2003.
[10] M. Rabin, Computable algebra, general theory and theory of computable fields, Trans. Amer. Math. Soc. 95 (1960) 341–360.
[11] L. Washington, Introduction to Cylotomic Fields, Grad. Texts in Math., vol. 83, Springer, 1982.
[12] K. Zahidi, Existential undecidability for rings of algebraic functions, PhD thesis, Ghent University, 1999.

Please cite this article as: J. Demeyer, Recursively enumerable sets of polynomials over a finite field, J. Algebra (2006), doi:10.1016/j.jalgebra.2006.09.030